

The Internet is Not Safe!

Twitter NathanHandler • Email nhandler@orchid.com



<https://archive.org/details/futurist19-theinternetisnotsafe>

The Internet is a fundamental part of our daily lives, but have you ever truly stopped to think about the cost you are paying for this service?

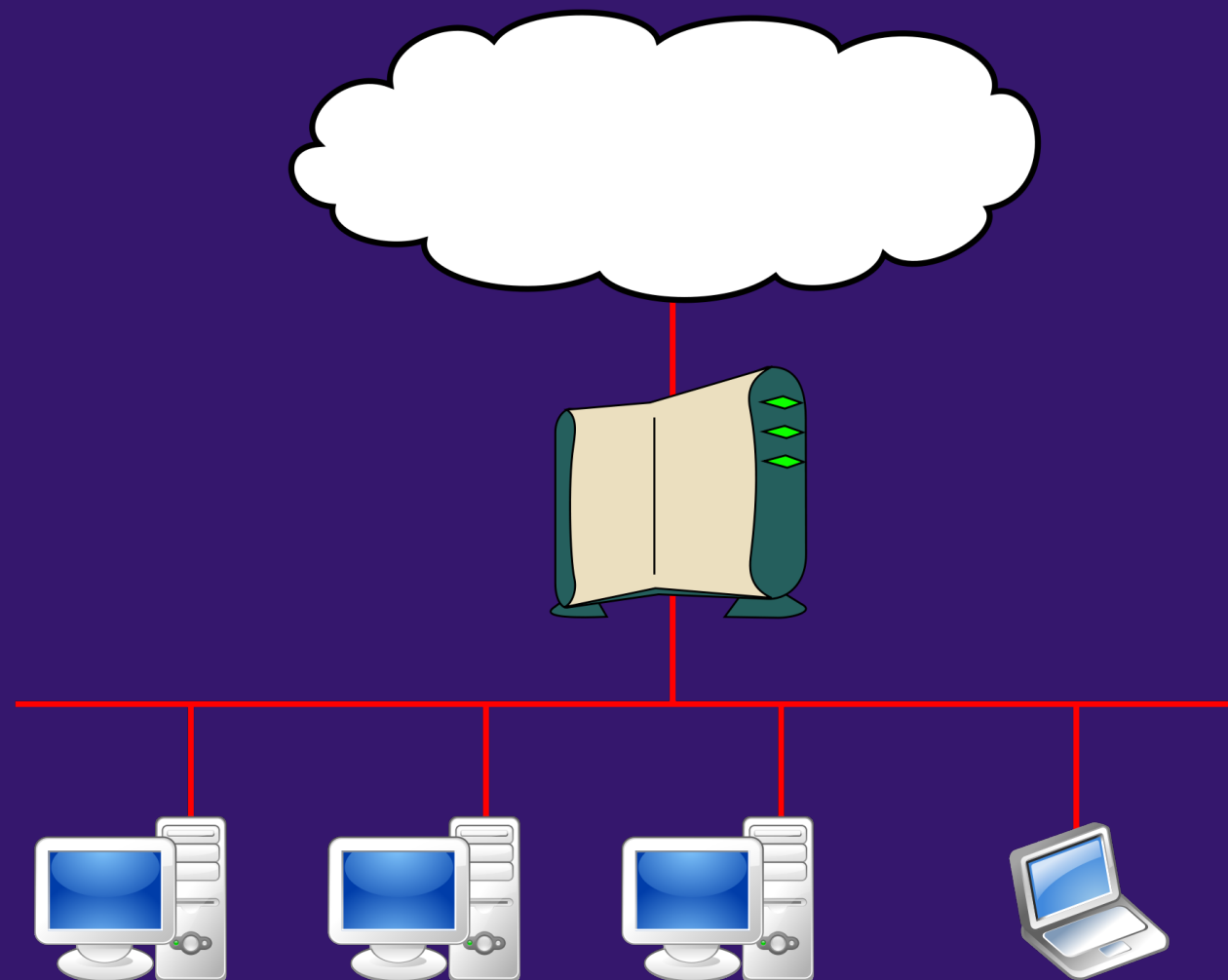
^ When the internet was created back in the '80s, it was designed as a means of connecting distributed groups of people and providing a means of communicating and sharing information.

^ It was not created with a goal of protecting user privacy

^ With things like frequent data leaks, GDPR, and Cambridge Analytica, it is more important than ever to understand how to protect our privacy in this modern era

^ To better understand this, let's take a quick look at what happens when you connect to the internet.

The Internet



Twitter NathanHandler • nhandler@orchid.com



<https://archive.org/details/futurist19-theinternetisnotsafe>

2

Most people are aware that their computer connects to their router and modem which then connects them to the internet where their favorite sites live

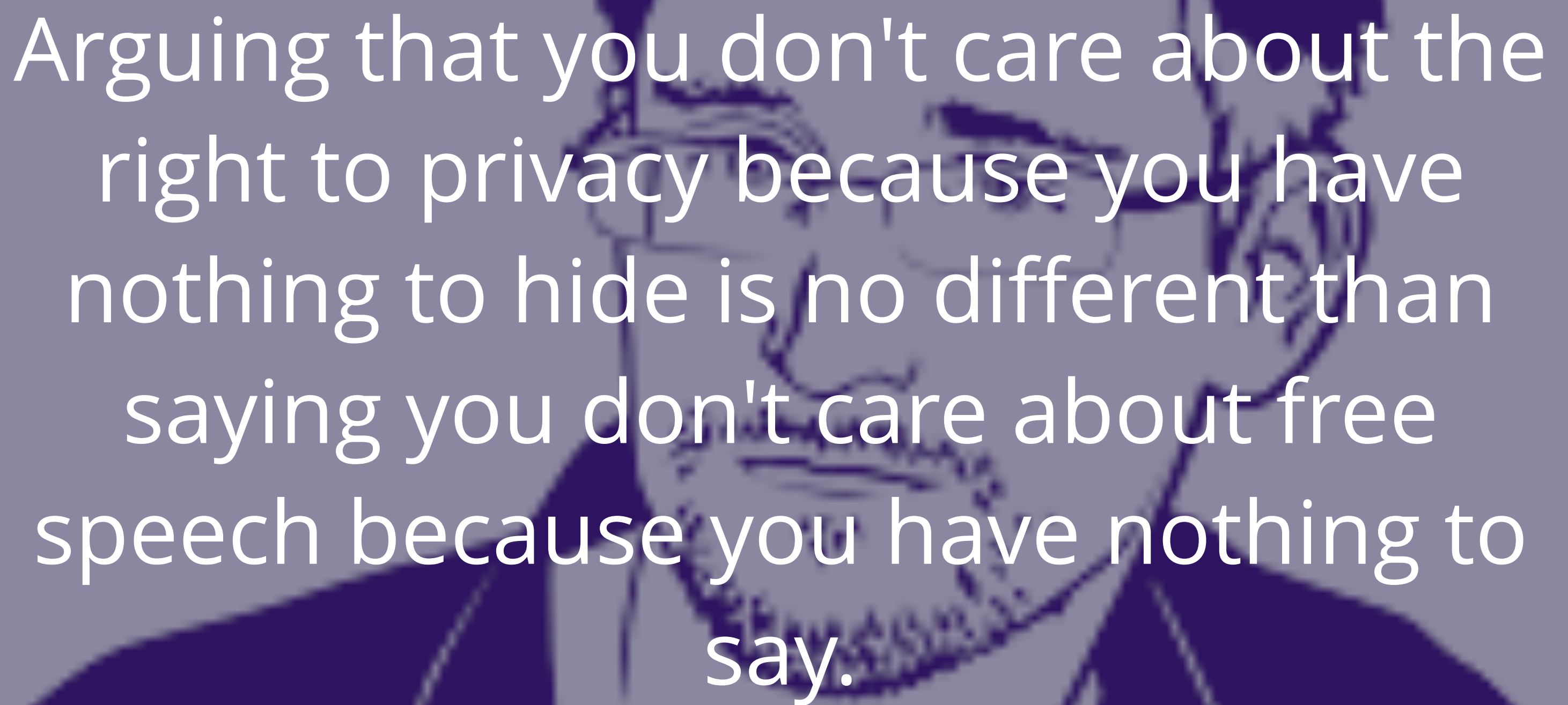
^ Since all of the computers are sending their traffic via the router, an evil coffee shop offering free wifi can easily see all of the websites being accessed

^ Or even if you are connecting from a trusted network, your ISP can still see what you are accessing

^ This can be problematic in a number of circumstances. Imagine looking up medical advice for a chronic illness that is plaguing you, only to later be fired from your job.

^ Or what if you are living in a country with an oppressive government that is attempting to identify and put a stop to all opposition? All of a sudden, being caught visiting certain websites could become a matter of life and death.

Or what if you simply want to stop your ISP from manipulating your web traffic to inject a banner displaying a notification about your account?



Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.

— *Edward Snowden*

Twitter NathanHandler • ✉ nhandler@orchid.com

 <https://archive.org/details/futurist19-theinternetisnotsafe>

3

A lot of you are probably sitting there thinking, "I'm just a regular old user with nothing to hide. Why should I care if someone knows that I bought a giant stuffed bear online?"

^ Once your data is out there, it is out there forever to be bought/sold and combined with other data sources to build up an even more complete profile of you.

^ If you still don't care about your privacy, do it for the people around you.

^ If only a small number of people are taking steps to protect their privacy, they will stand out as being "different" and attract attention.

^ We need to change the norm to be one of using safe browsing habits in order to protect those people who really need it.

Private Browsing



Twitter NathanHandler • nhandler@orchid.com



<https://archive.org/details/futurist19-theinternetisnotsafe>

4

Most popular browsers ship with a feature called *Private Browsing*

^ Despite its name, this feature will not protect your privacy in the situations being discussed

^ Private browsing doesn't expose your saved cookies/sessions and does not save visited websites to the browser's history

^ Your ISP and the websites you visit still see your traffic as usual

https://



An ever-growing number of websites support connecting in a secure and encrypted form using TLS

^ You can recognize one of these secure connections by the https:// bit at the start of the URL or the classic green lock icon (although this is changing in some browsers)

^ There are even web browser extensions such as "HTTPS Everywhere" by The Tor Project and the EFF that will attempt to force all connections to utilize this encryption.

^ This will prevent the coffee shop from seeing what you are sending, but they can still see where you are sending it to

^ This approach is also highly dependent on the website in question being capable of serving its contents over a secure connection

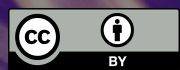
^ The main advantage of this approach is that it can be handled entirely server side without the need for users to install any additional software.

Proxies / VPN

Good Luck, I'm Behind 7 Proxies

— *4chan*

Twitter NathanHandler • nhandler@orchid.com



<https://archive.org/details/futurist19-theinternetisnotsafe>

6

So what can you do to conceal the sites you are visiting?

^ You can do what most people do and ask your favorite search engine.

^ When you ask Bing how to conceal your internet traffic, you will discover a plethora of free proxies and paid VPN solutions that promise to protect your privacy

^ A proxy is a server that you send your requests to which then forwards them on to the real site

^ The coffee shop owner will now see you connections going to the proxy instead of the real site

Proxies do not provide encryption and have to be configured for each application individually

^ So you better not forget about your email and chat applications

^ A VPN, on the other hand, will encrypt all traffic from your computer, but usage of these apps is sometimes blocked by governments

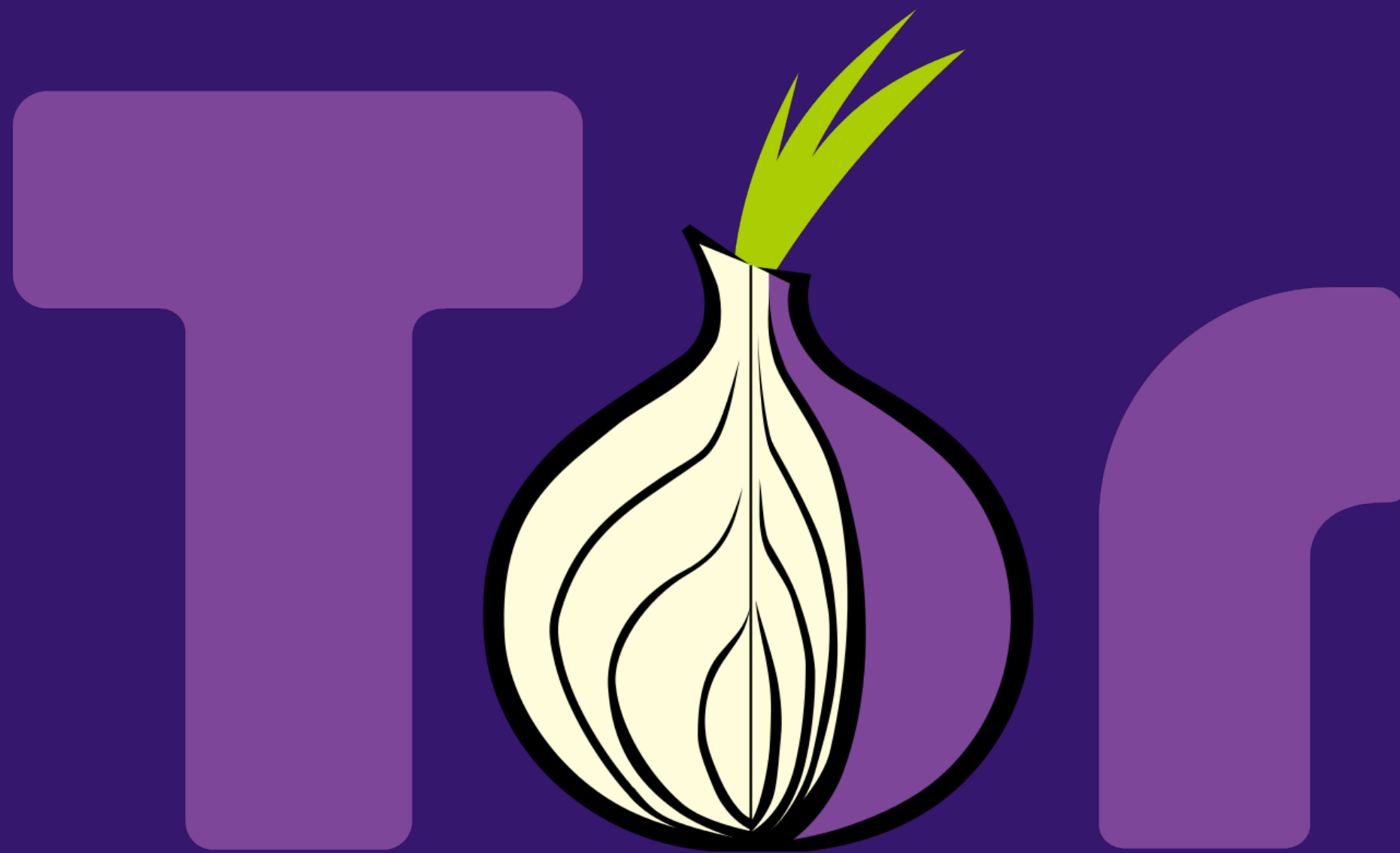
With both of these solutions, you are now sending all of your traffic to some random server, effectively placing all of your eggs in one basket

^ If they turn out not to be trustworthy, they might manipulate your traffic and steal your data.

^ Or if they are logging activity and get ordered to turn over the logs to the government, say good bye to your data.

Using multiple proxies, as in this famous 4chan quote, can be a means of ensuring no proxy knows both where you are connecting from and what site you are visiting, but once again, you better trust all of the proxies in the chain.

Tor



Twitter NathanHandler • Email nhandler@orchid.com



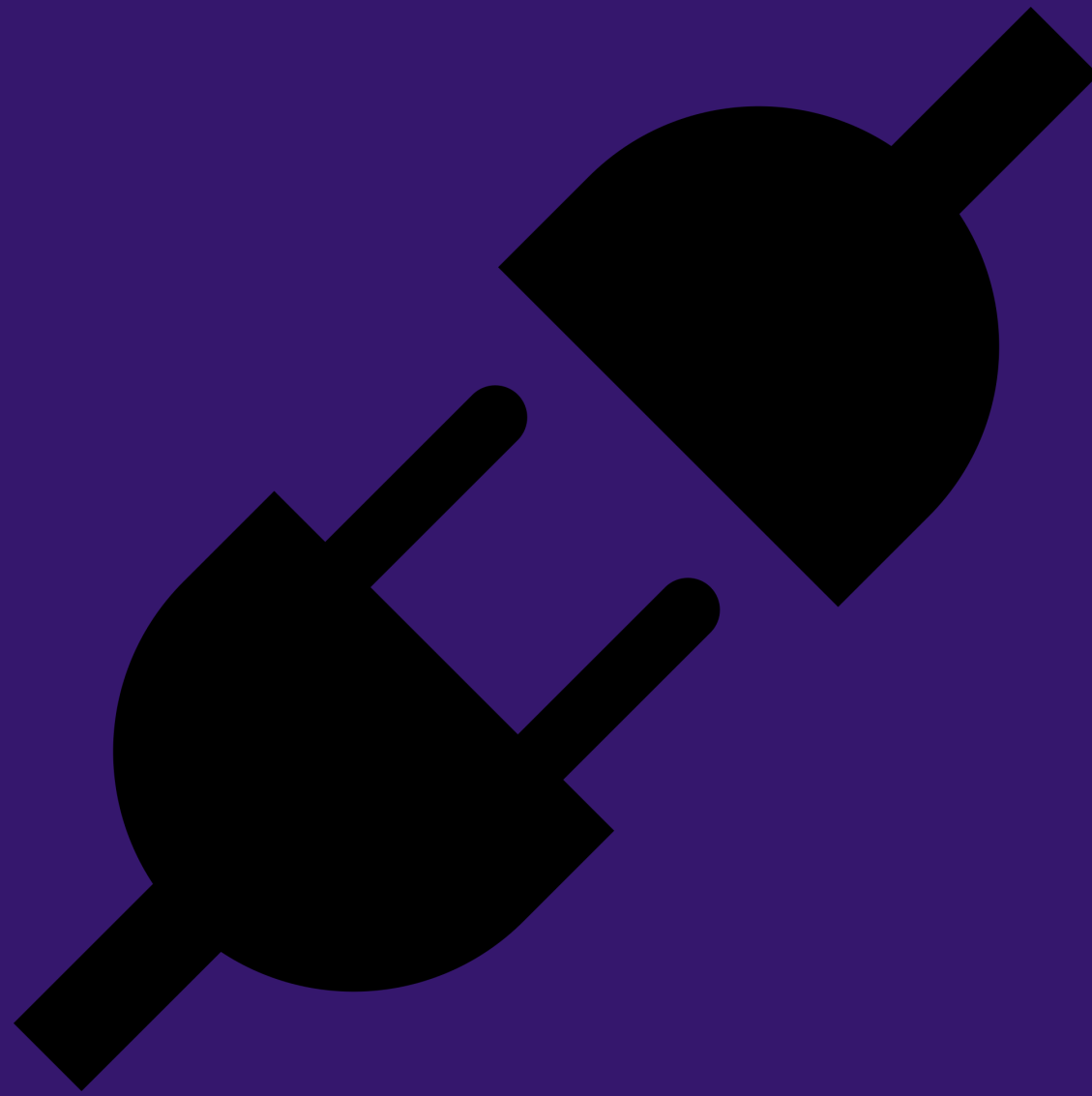
<https://archive.org/details/futurist19-theinternetisnotsafe>

7

Tor is a newer open source technology that takes the "7 Proxies" concept to the extreme

- ^ It will route your traffic securely through multiple relay nodes before ultimately sending the request to the final destination.
- ^ These nodes are located all over the world and run by many different individuals and groups. This means that even if one node is compromised, only a small amount of anonymous data is at risk.
- ^ A downside to the multiple relays and architectural design of Tor is that it can be quite slow, and is generally not recommended for use when performing actions like streaming Netflix.
- ^ Using Tor requires downloading and running a custom application
- ^ A combination of Tor and TLS encryption is one of the best options at present for preventing people from knowing the sites you visit
- ^ 9 Authoritative Directory Servers -->
- ^ No economic incentive to run nodes
- ^ No real control for node operators to control traffic (risky)

Plug-Ins



Twitter NathanHandler • Email nhandler@orchid.com



<https://archive.org/details/futurist19-theinternetisnotsafe>

8

Browser and website plug-ins are a common method of adding extra functionality

^ However, to add this functionality, they require access to the sites you visit and the data you send

^ This means an evil plug-in can easily steal your data and share it with an attacker

^ Closely audit the plug-ins you install and the permissions they are requesting.

^ If it sounds or looks suspicious, don't use it!

Tracking



Twitter NathanHandler • Email nhandler@orchid.com



<https://archive.org/details/futurist19-theinternetisnotsafe>

9

Even if you manage to hide the websites you are visiting, the battle is not over.

^ Many sites require you to login before you can interact with them or to bypass a paywall

^ Logging in immediately assigns an identity to all actions you take on the site.

^ If you login on multiple sites, tracking pixels and data exchange agreements can allow your identity on one site to be mapped to your identity on another site.

^ You can try to avoid logging in on sites, using fake one-time-use accounts, disabling javascript, and sending the Do Not Track (DNT) header

Solution?

- Completely **distributed and decentralized** Open Source solution
- **Impossible to censor** by a company/ISP/government without blocking large amounts of the internet
- Proper usage incentives and infinitely **scalable** to ensure long-term sustainability

orchid

-  www.orchid.com
-  OrchidProtocol
-  OrchidProtocol
-  Orchid-Labs
-  OrchidOfficial

 NathanHandler •  nhandler@orchid.com

 <https://archive.org/details/futurist19-theinternetisnotsafe>

10

Talking about a problem is one thing, but ideally, there would also be a viable solution available.

What would such a solution look like?

^ It needs to be completely distributed and decentralized.

As well as Open Source to facilitate auditing.

^ It must be impossible to censor, even by a government

^ And it needs to be scalable and have proper usage incentives to facilitate continued growth of a healthy system

^ If solving this problem sounds interesting to you, be sure to check out Orchid, where we are working to do just that.